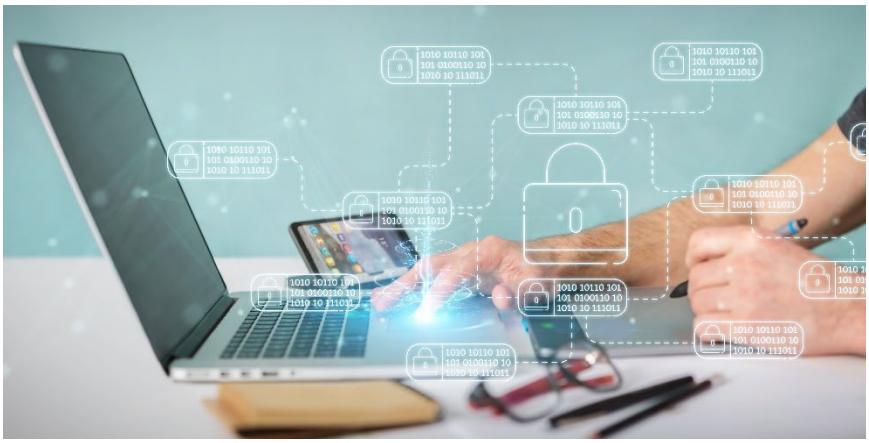
A-SIT

Zentrum für sichere Informationstechnologie - Austria

HANDLUNGSBEREICHE DIGITALE SOUVERÄNITÄT



Handlungsbereiche Digitale Souveränität

Autor:
Herbert Leitold, Arne Tauber, Peter Teufl
Mail: herbert.leitold@a-sit.at

Datum: August 2022

Abstract/Zusammenfassung:
Unter digitaler Souveränität wird die Möglichkeit verstanden, in der digitalen Welt selbstbestimmt und sicher zu handeln. Dies ist insbesondere für die öffentliche Verwaltung wesentlich, um ihre Aufgaben ungestört und unbeeinflusst effizient wahrnehmen zu können. Dazu ist es notwendig, strukturelle Abhängigkeiten, die Quellen einer Störung der Handlungsfähigkeit sein können, zuerst zu kennen, um sie dann systematisch zu verringern, Diese Ausarbeitung stellt dazu einen ersten Schritt dar, indem sie Ursachen struktureller Abhängigkeiten beschreibt und diese dann nach Bereichen kategorisiert darstellt. Es werden Möglichkeiten der Vermeidung von Abhängigkeiten aufgezeigt und ein Vorgehensvorschlag gegeben. Dabei ist das Ziel der Arbeit, den Diskurs zur Verbesserung digitaler Souveränität vorzubereiten, indem Handlungsmöglichkeiten aufbereitet werden, ohne solche tendenziös vorzuschlagen.

Inhalt

1. Einleitung

Abhängigkeiten reduzieren selbstbestimmte Handlungsfähigkeit. Rezent wurde dies in der Wirtschaft offensichtlich, wo Lieferkettenprobleme durch die Covid-19 Pandemie oder aus einer kurzen Blockade des Suezkanals zu weitgehenden Beeinträchtigungen führten, wobei aus Dominoeffekten dessen Ausmaß vorab kaum abschätzbar war. Eine drastischere Abhängigkeit in der physischen Welt wurde mit den Unsicherheiten der Erdgaslieferungen im Zuge der Ukrainekrise offensichtlich. Werden die Risiken aus solchen Abhängigkeiten schlagend, sind nicht nur einzelne Bertriebe oder Sektoren betroffen, sondern es kann auch die eigenständige Entscheidungshoheit staatlichen Handelns beeinflusst, das heißt die Souveränität beeinträchtigt sein.

Wie in der physischen können auch in der digitalen Welt Abhängigkeiten entstehen oder bereits bestehen, etwa aus Monopolen oder einfach aus dem Mangel an Alternativen zu einem wesentlichen System. In der bereits weitreichenden Notwendigkeit der öffentlichen Verwaltung, über funktionierende Informationstechnologie zu verfügen, ist die digitale Souveränität somit zunehmend von Bedeutung. Dabei hat der Begriff „Digitale Souveränität" eine gewisse Unschärfe, so zitiert eine aktuelle Schwerpunktstudie des deutschen Wirtschaftsministeriums aus 2021 über zwanzig Definitionen digitaler oder Technologie-Souveränität [1], die zwar ähnlich, aus dem Kontext aber durchaus auch unterschiedlich sind. Aus den Zielen dieser Arbeit scheint die Definition des deutschen Kompetenzzentrums öffentliche IT aus 2017 am zweckmäßigsten:

> *Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. [2]*

In dieser Ausarbeitung wird digitale Souveränität der öffentlichen Verwaltung in Österreich betrachtet. Ziel ist es, schädliche Abhängigkeiten aufzuzeigen, ihre Ursachen zu erfassen und Handlungsfelder zu beschreiben. Dabei wird noch kein konkreter Vorgehensvorschlag gegeben. Vielmehr soll das Dokument Entscheidungsträgern eine konzise Zusammenfassung wesentlicher, potentiell bestehender oder erwartbarer Abhängigkeiten geben, um den Diskurs zu deren Reduktion und Vermeidung zu unterstützen.

Die Arbeit ist dabei nicht isoliert erstellt, sondern berücksichtigt einschlägige andere Quellen, vor allem aus Deutschland, wo dieser Diskurs bereits im Gange ist und Vorarbeit besteht, etwa über eine für den Beauftragten der Bundesregierung für Informationstechnik durchgeführte, strategische Marktanalyse aus 2019 [3], die Beeinträchtigungen der digitalen Souveränität vor allem im Bereich der Software aufgezeigt hat, was 2020 über einen Beschluss der deutschen IT-Verantwortlichen der Ressorts zu Zielen und Handlungsfeldern zur Stärkung digitaler Souveränität geführt hat [4]. Diese Arbeit greift diese Vorarbeiten auf, übernimmt sie aber nicht einfach, sondern bezieht die österreichische Situation mit Initiativen wie dem Bundesclient mit ein. Sie berücksichtigt dabei auch Quellen, die breiter angesetzt sind, als reine Abhängigkeiten von Software, wie jene von Bitkom 2015 [5], oder die über die öffentliche Verwaltung hinausgehen, indem Empfehlungen für die Wirtschaft nach Anwendbarkeit bedacht werden, wie aus [1].

Es werden in Folge Ursachen von Abhängigkeiten in Abschnitt 2 noch abstrakt dargestellt. Diese werden in Abschnitt 3 auf konkrete technische Bereiche heruntergebrochen und erläutert, welche Vermeidungsstrategien jeweils möglich sind. Diese Vermeidungsansätze werden in Abschnitt 4 zusammengefasst, worauf in Abschnitt 5 ein Vorgehensvorschlag gegeben wird. Gesamt wird die Arbeit bewusst prägnant und konzise gehalten, um dem Ziel einer ersten Diskussionsbasis zur digitalen Souveränität zu genügen.

2. Ursachen struktureller Abhängigkeiten

Strukturelle Abhängigkeiten können aus harten, auf konkreten Entscheidungen festmachbaren Faktoren wie die Wahl eines bestimmten Produktes entstehen, das sich dominant in einer Organisation festsetzt, wie auch durch weichere Faktoren wie eine aus in Schulausbildung oder privatem Umfeld breit genutzte Umgebung, mit der hohes Wissen um deren Bedienung und Akzeptanz im beruflichen Umfeld einhergeht. Entsprechend können schädliche Abhängigkeiten über interne Gegebenheiten der Organisation, als auch über extern aufgeprägte Effekte getrieben sein, sowie eine Kombination dieser.

Dieser Abschnitt strukturiert solche Faktoren. Ziel ist die Frage zu beleuchten, warum es zu Abhängigkeiten kommt, noch nicht wo diese dann konkret auftreten. Es werden jedoch praktische und plakative Beispiele solcher Bereiche gegeben, wo eine Ursache einen Bereich besonders betrifft, um die abstrakte Darstellung der Quellen auch illustrativ mit deren Auswirkungen zu hinterlegen.

Die einzelnen Ursachen sind nicht für sich isoliert, sondern haben Querbeziehungen. So entstehen etwa sowohl Technologieführerschaft als auch Marktdominanz eines Herstellers aus dessen wirtschaftlichen Interessen. Sie werden hier aber getrennt betrachtet, zumal auch die Auswirkungen oder Strategien zur Vermeidung verschieden sind. Etwa kann und wird schädlicher Marktdominanz regulatorisch begegnet, die Innovationkraft oder Ertragsfähigkeit von Unternehmen üblicherweise nicht gesetzlich beschränkt.

2.1. Netzwerkeffekte

Unter Netzwerkeffekten wird eine Situation verstanden, wo sich der Nutzen eines Produkts erst mit dessen hoher Verbreitung einstellt, wie das Produkt über diese in Folge auch sekundären Nutzen gewinnen kann. Dabei kann Nutzen bei den Kundinnen und Kunden entstehen, wie etwa mit sozialen Netzwerken, wo der Austausch im privaten aber auch im beruflichen Umfeld erst Sinn macht, wenn man gewisse Verbreitung annehmen darf. Der Nutzen kann sich aber auf Seiten des Produkts und des Herstellers auch erst mit hoher Verbreitung einstellen. So wird ein Geschäftsmodell über werbe- oder Unternehmenskunden-finanzierte Suchmaschinen oder soziale Netzwerke erst wirksam, wenn damit eine große Zielgruppe erreicht wird. Sie ergeben sich auch nicht nur aus dem ursprünglichen Geschäftszweig einer Produktkategorie, sondern kann sich aus der Verbreitung zum ursprünglichen Einsatzgebiet sekundärer Zusatznutzen einstellen, so haben sich Mobiltelefone erst mit deren Ubiquität von Sprach- und einfacher Textkommunikation zur heutigen Vielfalt der Verwendung gewandelt.

Netzwerkeffekte sind in der Informationstechnologie häufig und entstehen bei für Anwenderinnen und Anwendern kostenlosen Diensten auch oft sehr rasch. Es ergeben sich daraus neben den Herstellern von Produkten für Dritte Vor- und Nachteile. Zu den Vorteilen zählen aus der breiten Verfügbarkeit Möglichkeiten, dies für eigene Angebote zu nutzen, sowie dass das Produkt Nutzerinnen und Nutzern schon vertraut ist und die Lernkurve der Verwendung schon durchlaufen wurde. Zu den Nachteilen zählt, dass sich Situationen massiver Marktdominanz entwickelt haben (z.B. Amazon im Onlinehandel, Google bei Suchmaschinen).

Die öffentliche Verwaltung partizipiert an der hohen Verbreitung von Produkten, indem sie diese für eigene Aufgaben nutzt. Dies ist etwa in der Kommunikation der Fall, wo soziale Medien konventionelle Formen längst ergänzt haben, aber auch als Teil der Strategie zur Erfüllung der Aufgaben, wie über die österreichische Mobile First Strategie Smartphones und Tablets als Zugangskanäle zu nutzen. Gleichzeitig ist die öffentliche Verwaltung nicht immer auch nur Akteur im Sinne des eigenen aktiven Aufgreifens neuer Technologie, aus einer hohen Verbreitung entsteht auch der Druck sowohl durch Bürgerinnen und Bürger, als auch der Mitarbeiterinnen und Mitarbeiter, diese Technologien einbeziehen und unterstützen zu müssen. Ein Beispiel ist Bring Your Own Device (BYOD), wo zunehmend eine Erwartungshaltung der Nutzung auch privater Gerätschaft gegeben ist.

2.2. Wirtschaftliche Interessen der Anbieter

Für Wirtschaftsunternehmen ist es ureigenes und legitimes Interesse, zu verkaufen, seine Marktposition auszubauen und langfristige, wirtschaftliche Beziehungen zu sichern. Gegenüber Endanwenderinnen und Endanwendern versuchen damit Hersteller einen hohen Verkaufserfolg und möglichst hohen Marktanteil zu erhalten. Bei institutionellen Kunden ist dabei oft nicht der einmalige Verkauf im Vordergrund, sondern mit einem Interesse an der langfristigen Bindung an das Produkt oder den Hersteller verbunden.

Für die öffentliche Verwaltung kann eine breite Nutzung eines Produkts indirekten Einfluss ausüben (vgl. Netzwerkeffekte in Abschnitt 2.1 davor), hinsichtlich potentiell schädlicher Abhängigkeiten ist aber das Bestreben der Hersteller nach langfristiger Bindung beachtlicher, das mit sogenannten „Lock-Ins" zu einer nachteiligen, weil bei starker Verankerung in wesentlichen Abläufen oder Leistungen einer Organisation nur mehr schwer zu lösenden Dependenz führend. Es werden hier deshalb vor allem Ursachen solcher Lock-Ins betrachtet, die von Herstellern durchaus auch bewusst eingesetzt werden, um den Ausstieg aus einem Produkt, wenn schon nicht zu verunmöglichen, zumindest zu erschweren und damit Bewahrungsdruck aufzubauen.

Technische Ursachen für Lock-Ins sind vor allem proprietäre Schnittstellen oder Formate, wie auch ein zwar grundsätzliches Halten an einschlägige Normen und Standards, jedoch unter Nutzung möglicher Erweiterungen oder Optionen in einer Art, dass dieselbe Funktionalität mit alternativen Produkten nicht immer möglich ist. Es ergibt sich daraus Aufwand im Wechsel zu alternativen Produkten, der bei proprietären Formaten sehr hoch sein kann, in der Kompatibilität zu Standards oft nicht vorab bestimmbar, sondern erst im konkreten Erproben absehbar wird.

Technisch-organisatorisch sind die Querbeziehungen von Produkten eines Herstellers zu nennen, wo sich aus der Integration verschiedener Anwendungen, die von einem Hersteller homogen integriert sind, ein Zusatznutzen ergibt. Beispiele wären bei Microsoft die nahtlose Integration von Active Directory oder Hello in die Produkte, oder die Verbindung von Mail, Kalender und Teams in Outlook. Ähnlich integrieren Google Dienste und Android über bestehende Anmeldung an einem Google Account optimal, ebenso sind Apple-Produkte homogen miteinander kompatibel. Verbreitete Produkte wie Active Directory oder Outlook sind zwar insofern offen, als über bekannte Schnittstellen oder Plugins breit genutzte Funktionen wie Single Sign-On oder das einfache Einladen einer Teams-Besprechung aus dem Kalender mit Alternativen möglich sind, schon Aufwand für Analyse oder Unsicherheiten zur tatsächlichen Kompatibilität im Betrieb schaffen aber Anreize homogener Landschaft des einen Herstellers und damit gewissen Bewahrungswunsch.

Eine weitere Lock-In Quelle technisch-organisatorischer Natur ist der Druck marktdominanter Hersteller von On-Premise auf Cloud-Lizenzierungsmodelle. Diese führen zwar einerseits bei institutionellen Kunden zur Suche nach On-Premise Alternativen, etwa aus Sicherheits- oder Compliance-Überlegungen (vgl. Abschnitt 2.4), und scheinen damit als Argument der Vermeidung von Lock-Ins tauglich. Wird der Schritt zu Cloud-Lösungen aber einmal gegangen, sei es über externe Plattformen wie Office365 oder über Betrieb eines Produkts auch in eigener Umgebung, ist aus der höheren Komplexität der geteilten Cloud-Produkte selbst und den nur für große Anbieter gegebenen Skaleneffekte eine Marktverengung auf eben diese marktdominanten Akteure wahrscheinlich.

Wirtschaftlich kann ein Lock-In über den Abtausch attraktiver Einstiegskosten gegen höhere im Betrieb initiiert werden, wenn letztere und Erweiterungen in der Praxis nur vom selben Anbieter durchführbar sind. Im Bereich der Konsumprodukte ist dies mit billigen Druckern als attraktiver Einstieg und entsprechend teureren Patronen für den laufenden Betrieb bekannt. Bei institutionellen Kunden sind vor allem Standardprodukte, die relativ günstig angeboten werden, dann aber maßgeschneidert und nicht auf Alternativen übertragbar angepasst werden, Ursache langfristiger Bindung. Dem wäre bei Office Produkten intensiver Einsatz von Makros vergleichbar die, wenn dezentral erstellt aber betriebswichtig

eingesetzt, nicht einfach übertragbar sind und Gegendruck zu Alternativen ergeben. Solcher Portierungsaufwand ist etwa im Bundesclient oder STAB-Arbeitsplatz Teil der Überlegungen.

Druck auf den betrieblichen Einsatz eines Produktes entsteht auch durch hohe Verbreitung, wo seitens der Hersteller hohe Durchdringung durch relativ günstige oder kostenlose Versionen für das private Umfeld oder für Schulen induziert wird. Dies bewirkt noch keine Lock-In Effekte im eigentlichen Sinn, es beeinflusst aus der Erwartungshaltung von Mitarbeiterinnen und Mitarbeitern, ein verbreitetes und bekanntes Produkt auch im beruflichen Umfeld vorzufinden, wie mit der Bekanntheit aus Kostenvorteilen geringeren Schulungs- oder Fehlbedienungsaufwands die Entscheidung für ein Produkt.

2.3. Technologieführerschaft und -herkunft

Kerntechnologien der Informationstechnologie sind nicht oder nicht mehr europäischer Provenienz. Von einigen Ausnahmen wie SAP als Marktführer zu Enterprise Resource Planning abgesehen, sind Hardware wie PCs, Server oder Mobiltelefone, Betriebssysteme wie Windows, iOS oder Android, Cloud Hyperscaler wie Amazon Web Services oder Google, oder Software im Office-Umfeld aber auch für Server von USA oder Asien dominiert. Es ergeben sich daraus Abhängigkeiten die sich oft auf liberale Märkte in klar demokratischen Strukturen beziehen, aber auch zu Umgebungen mit staatlichem Einfluss aus autoritärem bis zu totalitärem Umfeld reichen können.

Die öffentliche Verwaltung muss bei materiellen Gütern die ausreichende Verfügbarkeit bedenken, wo rezente Lieferkettenprobleme vor allem auch bei Prozessor- oder Controller-Chips die Lieferzeiten und Ersatzteile bei PCs und Severn betroffen haben. Ergänzt um immaterielle Güter wie Software oder Cloud muss die öffentliche Verwaltung sowohl die Informationssicherheit wie Konfidenz in die Funktion und das Fehlen von geheimdienstlichen Einfalltoren, die Einhaltung rechtlicher Rahmenbedingungen wie des Datenschutzes, aber auch die weitere Verfügbarkeit in Krisensituationen berücksichtigen.

Ein weiterer Faktor, der Abhängigkeit fördert, ist, wenn sich einzelne Akteure einen Technologievorsprung erarbeitet haben, der oft bis zu mehreren Jahren betragen kann. Dies ist insbesondere in Infrastrukturelementen kritisch, wo in einer Erneuerung Druck besteht, die aktuell leistungsfähigste Technologie anzuschaffen, singuläre Anbietersituationen aber Monopole fördern können. Solche Technologieführerschaft war bei Internet Core- und Edge-Routern lange über Cisco gegeben, wo die Dominanz aber mittlerweile geringer wurde und Alternativanbieter schon relevante Marktanteile haben. Aktuell wird bei 5G Huawei ein signifikanter Technologievorsprung zugesprochen. Lässt sich ein Technologievorsprung halten und damit Marktdominanz erreichen, erschwert es Alternativen, in den Markt einzutreten oder sich zu behaupten, was wiederum in eine Abhängigkeit von einzelnen oder nur wenigen Anbietern führt.

Mit nicht-europäischer Technologie-Dominanz geht einher, dass die Technologiegestaltung weniger beeinflussbar und eigene Ansätze weniger durchsetzbar sind. Beispiele sind die NFC-Schnittstelle in iPhones, deren Nutzung lange nicht möglich war, oder der Ansatz qualifizierter Webserverzertifikate aus der eIDAS Verordnung, die zwar Haftungs- und Sicherheitsnormen dem europäischen Rechtsraum unterordnen, mangels Unterstützung der wesentlichen Web-Browser aber keine praktische Relevanz erhalten haben, damit in kritischen Anwendungen auch nicht vorgeschrieben werden können.

2.4. Kosten- und Marktdruck

Hochskalierende Standardanwendungen haben in der Cloud einen Kostenvorteil gegenüber spezifischen und lokalen Lösungen. Das trifft sowohl auf Grundfunktionen wie Speicher, Applikationsserver oder Email zu, wie auch auf komplexere Anwendungen wie Office-Lösungen. Es entsteht ein Kostendruck, der zwar immer auch im Konzert mit anderen Anforderungen wie Informationssicherheit, Datenschutz oder Datenhoheit zu sehen ist, sich für die öffentliche Verwaltung getrieben von stärkerer Cloud-Nutzung in der Wirtschaft oder durch Cloud-Initiativen anderer Staaten aus deren Beispielwirkung auch erhöht.

Migrationsdruck entsteht nicht nur über Kosten, sondern auch funktional. So ist kollaboratives Bearbeiten von Dokumenten in Cloud-basierten Office-Paketen integraler Bestandteil des Leistungsumfangs, was mit lokalen Office-Installationen erst über Umwege wie Plugins zu gemeinsamem Speicherort wie in Teamrooms oder über zusätzliche Web-Anwendungen wie OnlyOffice gesondert bereitgestellt werden muss.

Eine Abhängigkeit entsteht noch nicht notwendiger Weise aus einem Wechsel in die Cloud, sondern daraus, dass sich wesentliche Skalen- und damit Kosteneffekte vor allem für Hyperscaler einstellen. Es kann damit zu einer Verengung der Anbieter kommen, wo mit funktionalen Zusätzen wie kollaborative Bearbeitung Anbieter wie Microsoft mit Office365 oder Google mit docs, die jeweils auch solche Hyperscaler sind, ihre dominanten Positionen halten oder weiter ausbauen können.

2.5. Nutzungsgewohnheiten, Fähigkeiten Anwender*innen

Bei PC-artigen Endgeräten besteht seit längerem faktische Hegemonie über Microsoft Windows als Betriebssystem, in den Office-Produkten klare Dominanz von Microsoft Office. Alternativen wie Linux oder quelloffene Software-Pakete wie LibreOffice bzw. Web-Alternativen wie Google docs bestehen, sind mit jeweils einstelligem Marktanteil noch deutlich hinter Microsoft von noch immer über drei Viertel der Installationen in Europa.

Im Mobilbereich haben sich die Plattformen auf Android und iOS eingeengt, zumindest in Europa wo Varianten wie Huawei Harmony derzeit geringe Rolle haben. Es ist mobil das Nutzungsverhalten im Vergleich zu PCs über eine höhere Anzahl an spezifischen Apps von jeweils geringerer Funktionalität, als dies typische PC Programme haben, doch anders. Auch sind die den Nutzerinnen und Nutzern vom Betriebssystem angebotenen Funktionen typisch weniger mächtig und daraus intuitiver. Es kann aber auch hier davon ausgegangen werden, dass einer breiten Masse an Anwenderinnen und Anwendern die Bedienung beider Mobil-Betriebssysteme schon aus dem privaten Gebrauch vertraut ist.

Bestehen solch dominante Situationen längerfristig, bestimmen sie sowohl die von Anwenderinnen und Anwendern erwartbaren Fähigkeiten im Umgang, auch zielt die Ausbildung wie etwa zu Computer-Grundkenntnissen darauf ab. So ist die Nutzung von Microsoft im Schulbetrieb üblich, Grundkenntnisse zu den Produkten ist Bestandteil etwa des Computer-Führescheins ECDL. Die Dominanz wird auch vom Hersteller über günstige Pakete für Schulen oder Schülerinnen und Schüler gestützt.

In der Bevölkerung verankerte breite Fähigkeiten im Umgang mit Produkten sind im betrieblichen Einsatz ein Vorteil, da sie Schulungsaufwände gering halten bzw. Kenntnisse schon in der Einstellung neuer Mitarbeiterinnen und Mitarbeiter erwartbar sind. Gleichzeitig beeinflusst dies die Entscheidung für ein Produkt, was wiederum dieses weiter verankert und somit bestehende Kenntnisse des Personals Gegendruck zum Abbau vorhandener Abhängigkeiten aufbauen.

2.6. Verwaltungsinterne Faktoren

In der Betrachtung von Abhängigkeiten der öffentlichen Verwaltung ist dessen spezifische Situation zu bedenken. Ein Spezifikum ist, dass die öffentliche Verwaltung Regularien produziert, Informationen hält und verarbeitet, oder aus seinen Aufgaben Bürgerinnen und Bürgern sowie Unternehmen Dienstleistungen anbietet, aber – wie auch die meisten Betriebe – typisch nicht selbst Produzent aller benötigter Informationstechnologie ist. Es sind aber für dessen Konzeption und Einsatz Kompetenzen notwendig, die entweder intern gehalten oder extern bezogen werden müssen.

Die öffentliche Verwaltung wie auch die nahestehenden Dienstleister in der Informationstechnologie wie das Bundesrechenzentrum BRZ stehen unter Einsparungsdruck. Gleichzeitig ist Mangel an IT-Fachkräften offensichtlich und wird erwartbar längerfristig anhalten. Die öffentliche Verwaltung steht dabei im

Wettbewerb zum privaten Markt und es kann zusehends schwieriger werden, notwendige digitale Kompetenzen in Spitzenqualität selbst aufzubauen oder intern zu halten.

Können qualitative digitale Kompetenzen nicht intern gehalten werden beziehungsweise, wie aus der Dynamik der Informationstechnologie laufend notwendig, immer wieder erneuert und weiter ausgebaut werden, sind sie extern zu beziehen. Als ohnehin größter Auftraggeber stellt die Beschaffung externer Kompetenz noch keine strukturelle Einschränkung der Eigenständigkeit der öffentlichen Verwaltung dar. Wo sich dies aber in eine Abhängigkeit entwickeln kann ist, dass extern bezogene Kompetenz nicht immer unabhängig und nicht notwendigerweise ohne Eigeninteressen ist. Die Herausforderung ist hier, in der Beratung und Konzeption von Vorhaben nicht durch etwaige die Beratenden überlagerte Interessen in Entscheidungen zu gehen, die bei Vorhandensein ausreichend interner oder unabhängiger externer Kompetenz anders getroffen würden.

Aus dem Kostendruck sowie aus knappen Ressourcen besteht eine Tendenz weg von Eigenentwicklung hin zum Einsatz von Standardprodukten. Wenn dies auch Vorteile wie in der längerfristig erwartbar gesicherten Wartung und Weiterentwicklung dieser Standards haben kann, kann es Kompromisse in der Funktionalität bedeuten, die dann nicht umsetzbar oder nur aufwändig erweiterbar sind. Vor allem können sich aber Abhängigkeiten von derart entwickelten Erweiterungen bis zum Lock-In ergeben (vgl. Abschnitt 2.2).

Ein weiteres Spezifikum der öffentlichen Verwaltung ist dessen verschiedene Ebenen und föderale Strukturen, wo aus den zugeordneten Verantwortungsbereichen eigenständig entschieden wird. Werden Ansätze zur Reduktion von Abhängigkeiten und damit zur Stärkung digitaler Souveränität entwickelt, sollten diese auch von allen Verwaltungsebenen sowie Mitarbeiterinnen und Mitarbeitern mitgegangen werden. Abbau von Abhängigkeiten bedarf auch Transformation, diese sowie damit einher gehende Innovation muss von allen Ebenen getragen werden. Tendenzen der Bewahrung können innovationsfeindliches Umfeld nähren, was den Handlungsspielraum auf den Bestand verengt und damit Abhängigkeiten festigen kann.

3. Bereiche struktureller Abhängigkeiten

Abhängigkeiten können in verschiedenen Ebenen und Komponenten eines digitalen Dienstes bestehen. Es macht Sinn, diese gesondert zu betrachten, da je nach Element unterschiedliche Strategien zu Abbau oder Vermeidung erfolgsversprechend sind. Beispielweise hat Österreich in der Informationssicherheit oder im E-Government die wissenschaftlichen und operativen Ressourcen, Dienste selbst entwickeln zu können und Abhängigkeiten gering zu halten. Für Endgeräte-Hardware oder deren Komponenten wird signifikante Reduktion der Abhängigkeit von asiatischen Chipherstellern über eigene Produktion kaum gelingen und, wenn überhaupt, wohl nur in gesamteuropäischer Anstrengung realistisch zu vermindern sein. In anderen Bereichen wie der Office-Software kann dies auch über Anlehnung an Aktivitäten anderer Staaten gelingen, wie es über die deutsche dPhoenix Suite in Österreich zum Bundesclient erprobt wird.

In diesem Abschnitt werden deshalb Bereiche beschrieben, in denen Abhängigkeiten bestehen, bestehen könnten, oder noch nicht kritisch bestehen aber sich potentiell dahin entwickeln könnten.

3.1. Hardware-Plattformen

In der öffentlichen Verwaltung zur Informationstechnologie eingesetzte Hardware ist sehr breit und reicht von Geräten der Endanwenderinnen und Endanwender wie PCs, Laptops, Tablets oder Smartphones, spezifische Komponenten wie Dienstkarten, bis für Anwendungen eingesetzte Server oder Infrastrukturkomponenten wie Firewalls, Router oder Switches.

In diesem Bereich und bei den genannten Komponenten sind, von spezifischen Ausschreibungen wie die Dienstkarte abgesehen, keine Abhängigkeiten von nur einzelnen Herstellern oder Lieferanten gegeben, es gibt vielmehr unterschiedliche Bezugsquellen etwa aus den Angeboten der BBG. In spezifischen Infrastrukturbereichen wie Internet Core Routern oder bei starker Technologieführerschaft kann es eine Einengung auf relativ wenige Anbieter geben, jedoch bestehen kaum klare Monopolstellungen.

Betrachtet wird der Bereich Hardware hier jedoch nicht zuletzt aus den jüngsten Erfahrungen der Lieferkettenprobleme mit der Covid-19 Pandemie oder der kurzzeitigen Blockade des Suez-Kanals. Aus der Vielzahl der Komponenten wie Leiterplatten und Chips oder deren Rohstoffe lassen sich mögliche Engpässe nicht an einem einzigen Element festmachen. Wenngleich hier einiges an Industrie in Österreich und Europa besteht, ist vor allem eine Abhängigkeit von asiatischer Chip-Fabrikation gegeben.

Für Infrastrukturkomponenten sind geheimdienstliche Einfallstore über Hardware-Trojaner oder verdeckte Funktionen der etwa bei 5G oder Routern doch komplexen Firm- und Software nicht auszuschließen. Dies ist zwar keine direkte Abhängigkeit, werden jedoch Hersteller aus Bedenken nicht berücksichtigt, wie der Ausschluss von Huawei im 5G-Aufbau in einigen Staaten, verengt sich die Zahl der Anbieter, was bei beschränktem Markt indirekt eine Anhängigkeit von diesen induzieren kann.

Mitigation des Ausfalls eines Lieferanten oder Herstellers ist in Standardprodukten durch vitalen Markt vieler Anbieter und damit alternativen Lieferanten etwa aus den BBG-Katalogen gegeben. Abhängigkeit von nicht-europäischen Herstellern von Komponenten, insbesondere bei Prozessoren und Controllern, lässt sich aus Vielfalt und Volumen nicht in Österreich allein begegnen und kann, sofern aus der Breite an Anbietern überhaupt als bedrohlich angesehen, bei als wesentlich gesehenen Technologien nur eine Frage gesamteuropäischer Industriepolitik sein. In den notwendigen Rechenressourcen scheint bei längeren Lieferengpässen oder Netzwerkausfällen (vgl. Abschnitt 3.4) regional erreichbare Cloud- oder Rechenzentren-Infrastruktur eine plan- und steuerbarere Überbrückungsstrategie, als ein wenig realistischer Ansatz autarker Produktion von Massenkomponenten.

Fragen der Sicherheit von Infrastruktur-Hardware sind weniger einer Abhängigkeit von Produkten oder Herstellern zuzuordnen, als dass sie in kritischen Elementen eine von entsprechenden Kriterien der Beschaffung bzw. der Prüfung oder Zertifizierung der Produkte ist.

3.2. Betriebssysteme

In den Betriebssystemen der Endgeräte sind mit Windows bei PCs und Laptops bzw. mit iOS und Android klare Hegemonie-Situationen gegeben. Es ist hier weniger der Ausfall eines Herstellers oder dessen Liefereinschränkungen zu bedenken, sondern die Dominanz der Funktionalität und aus der Marktmacht ein Aufzwingen von Lizenzbedingungen.

Hier nicht gesondert betrachtet wird macOS bei Apple Produkten. Dies da mit hinreichender Abstraktion macOS ähnlich wie Windows als ein für eine Hardware-Plattform dominante, aber durch andere Betriebssysteme ersetzbare Situation darstellt. Es wird damit für PCs nur die verbreiterte Situation Windows betrachtet. Das gesagte ist auf macOS anwendbar, wobei aus geringerer Durchdringung Überlegungen zur allgemeinen Vertrautheit der Bedienung entsprechend weniger zutreffen.

In der Informationssicherheit ist geheimdienstlicher Einfluss auf die Hersteller nie ganz ausschließbar. Mit der Ubiquität der Systeme und daraus breiter Prüfung etwa durch die Wissenschaft tritt das Risiko bewusst eingebrachter Einfallstore hinter aus sogenannten Zero-Day Exploits ohnehin anzunehmende und von unfreundlich agierenden staatlichen oder gut organisierten Gruppen ausnutzbare Schwachstellen (vgl. etwa Bekanntmachungen von genutzten Schwachstellen durch Edward Snowden).

Der Abhängigkeit von PC-Betriebssystemen kann man über Alternativen begegnen, wie mit Linux als Open Source Arbeitsplatz. Erfahrungen dazu gab es im breiteren Maßstab etwa mit Linux für München

(LiMux), wo ab 2006 Windows auf mehr als Zehntausend Arbeitsplätzen auf Open Source umgestellt und in der Evaluation Einsparungen und breitere Softwareauswahl berichtet wurden. 2017 wurde jedoch eine Rückkehr zu Windows beschlossen, um 2020 wieder auf eine Open Source Strategie geändert zu werden. Es sind hier keine einfachen, nur eindimensionalen Kriterien wie Kosten oder Abhängigkeit von einem Hersteller anwendbar, vielmehr sind aus der starken Verbreitung auch Netzwerkeffekte oder Vertrautheit der Nutzerinnen und Nutzer zu bedenken (vgl. Abschnitt 2.1 und Abschnitt 2.5).

Auf den ersten Blick ist eine Entscheidung zwischen kommerziellem Windows und quelloffenen Linux-Varianten in der PC-Welt der Situation der dominierenden Mobil-Plattformen iOS als geschlossenes Produkt und Android als quelloffen ähnlich. Es unterscheidet sich das mobile Umfeld aber grundsätzlich dadurch, dass PCs eine weitgehend gemeinsame Architektur haben, Mobilgeräte stärker vom Hersteller abhängig sind und daraus der Hardware-Hersteller auch das Betriebssystem im Allgemeinen nicht ersetzbar vorgibt. Angestrebter Ersatz des Betriebssystems würde in mobilen Umgebungen daher meist Ersatz der Geräte bedeuten. Ein bei Mobilgeräten besonderer Aspekt ist jedoch, dass die von Herstellern garantierten Aktualisierungen oft nur relativ kurz und auch unter der eigentlichen Lebensdauer des Geräts selbst liegen. Dies mag aus der im Privatbereich relativ geringen Behalte-Dauer von Handies samt Degradation der Nutzbarkeit über Akkulaufzeit oder einer steigenden Leistungsanforderung von Apps und damit ohnehin rascherem Austausch sekundär anmuten, stellt aber insofern eine Einschränkung digitaler Souveränität im Sinne dieser Arbeit dar, als aus den für die Informationssicherheit notwendigen Aktualisierungen der Verwaltung ein Wechsel sonst noch funktionsfähiger Geräte aufgezwungen oder diese über längere Update-Garantien für high-end Geräte in ein teureres Segment gedrängt wird.

In den, abgesehen von vorgenannter Update-Situation im Mobilbereich, breit eingesetzten, getesteten und gewarteten Betriebssystemen ist in den wesentlichen Vertretern, d.h. Windows, macOS, Linux, iOS und Android von vergleichbarer, dem Stand der Technik entsprechender Informationssicherheit auszugehen. Es wird hier deshalb die Wahl des Betriebssystems aus dem Blickwinkel der Informationssicherheit keine Rolle als Mitigator von Abhängigkeiten zugemessen. Vielmehr wird in allen Situationen von noch weiteren Maßnahmen auszugehen sein, wie Endgeräteschutz, Verschlüsselung des Dateisystems, VPN, gemanagte Systeme oder Zero Trust Ansätze.

3.3. Anwendungs-Software

Der Bereich der Anwendungs-Software ist naturgemäß sehr breit, es lassen sich jedoch Funktionsblöcke festmachen, die an praktisch allen Geräten im beruflichen Einsatz verwendet sind. Dies sind Office-Pakete zur Textverarbeitung, Tabellenkalkulation und für Präsentationen, Web-Browser, Email-Clients isoliert oder in Groupware zusammen mit Kalender und Adressverwaltung, sowie nicht zuletzt seit Home-Office durch die Covid-19 Pandemie Videokonferenzpakete (letztere sind gesondert in Abschnitt 3.6 behandelt).

In den Office Paketen dominiert Microsoft bzw. zum PDF-Format Acrobat Adobe, letzteres für die Grundfunktonen in einer kostenlosen Version. Beide Hersteller drängen in den Lizenzmodellen von Kauf-Versionen mit lokaler (on-premise) Installation auf Mietmodelle in der Cloud. Es ergeben sich daraus sowohl Fragestellungen des Wechsels von Einmalkosten auf laufende, als auch bei Nutzung öffentlicher Clouds aus der Verarbeitung als Dienstleister solche der Informationssicherheit und des Datenschutzes. Für die öffentliche Verwaltung sind mit Verarbeitung in der Cloud auch rechtliche Fragen wie der CLOUD Act bemerkenswert, der die Datenhoheit in Frage stellt, nachdem US Behörden Zugriff auf Daten durch die genannten, amerikanischen Hersteller zu gewähren wäre.

In der Groupware ist Microsoft Outlook verbreitet, wenngleich als Email-Client keine wie bei Microsoft Office erreichte Dominanz gegeben ist. Als Abhängigkeit ergibt sich weniger die Kernfunktion Email, wo aus dem hohen Standardisierungsgrad Alternativen sowohl bei Clients als auch Servern vielfältig sind, als die Groupware-Zusatzfunktionen des Exchange-Servers, wie Kalenderfreigaben, Gruppenkalender oder

organisationsübergreifende Adressbücher. Über eine proprietäre Schnittstelle hat sich bei Microsoft Exchange ein gewisses Maß an Lock-In entwickelt, was einen Wechsel aufwändiger macht.

Hoher Standardisierungsgrad und damit Alternativen sind auch bei Web-Browsern gegeben. Die wesentlichen Hersteller sind jedoch nicht-europäisch. Dies ist insofern bemerkenswert, als damit auch die Funktion nicht-europäisch determiniert wird und europäische Ansätze wie Unterstützung qualifizierter Webseitenzertifikate aus der eIDAS Verordnung dem Wohlwollen der Hersteller untergeordnet ist, wo eine Unterstützung am konkreten Beispiel bisher nicht gegeben ist. Das Beispiel mag nicht als kritisch im Sinne Erhalts der öffentlichen Aufgaben angesehen werden, dient aber der Illustration, dass selbstbestimmtes Handeln im Sinne der eingangs gegebenen Definition digitaler Souveränität auch dadurch beeinträchtigt ist, dass ausschließlich nicht-europäische dominierte Komponenten spezifisch europäische Interessen potentiell nicht unterstützen.

Im Mobilbereich ist die Situation insofern anders, als Apps schon aus den aus dem Formfaktor weniger mächtigen Eingabemöglichkeiten in der Funktionalität weniger umfangreich sind, für eine Funktion auch meist mehrere Angebote bestehen.

Mitigations-Strategie zur Abhängigkeit von Software ist der Einsatz von Alternativen, wo aus Überlegungen zu Lizenzkosten, Emanzipation von dominanten kommerziellen Herstellern, oder zu allfällig notwendiger Anpassbarkeit oft quelloffene Ansätze, das heißt Open Source Software, priorisiert wird. Zu den genannten Paketen wie Office, Email oder Webbrowser gibt es solche Alterativen. Diese sind in der Bedienung den dominanten kommerziellen Lösungen oft ähnlicher, als dies bei alternativen Betriebssystemen (vgl. Abschnitt 3.2) der Fall ist, womit Umstellung von vertrauter Bedienung der Mitarbeiterinnen und Mitarbeiter ein weniger starker Faktor ist. So kann ein Wechsel zu einem Open Source Textverarbeitungsprogramm mit ähnlichen Bedienelementen wie Microsoft Word der Umstellung auf eine neuere Version von Word ähnlich empfunden werden. Komplexer wäre jedoch die Portierung von in einer Organisation allenfalls intensiv genutzten Makros.

Ist man bei kommerziellen Anbietern von einem Unternehmen als Hersteller abhängig, das gerade bei dominanten und damit klar erfolgreichen Produkten schon aus wirtschaftlichen Überlegungen Interesse an langfristiger Stellung des Produkts am Markt hat, kann sich dies in der Open Source Welt gegen eine Abhängigkeit von der so genannten Community tauschen, also die eine quelloffene Software weiterentwickelnde und wartendende Gruppe, wo sich die Intensität der Betreuung auch bei einem erfolgreichen Produkts aus geringerem Interesse der Community reduzieren kann. Eine Degradation der Qualität oder ein Auslaufen des Produkts würde eine zuvor potentiell schädliche Abhängigkeit vom kommerziellen Anbieter durch ein anderes, letztlich aber vergleichbares Risiko geringer werdender Stützung des Open Source Produktes ersetzen. Dies wird unter anderem auch im Pilotprojekt zum Bundesclient unter Nutzung der deutschen Phoenix Suite berücksichtigt, wo in den wesentlichen Funktionen zwei alternative Open Source Quellen angestrebt sind. Solche Partizipation an Projekten mit allenfalls gemeinsamen Entwicklungen mehrerer Staaten bis hin zu gesamteuropäischen Lösungen können die Nachhaltigkeit eines Wechsels zu Open Source über Skaleneffekte stützen.

3.4. Netzwerke und Kommunikationsinfrastruktur

Moderne Informationstechnologie ist von Kommunikation geprägt. Diese ist gerade in der öffentlichen Verwaltung essentiell, wo Daten zwischen den Behörden und Verwaltungsebenen ausgetaucht werden. Die Bürgermeister als Meldebehörde und das Führen der lokalen Melderegister im ZMR mit den Autorisierungen aus dem Portalverbund sind nur eines der unzähligen Beispiele, wie abhängig eine funktionierende Verwaltung von technischen Netzwerken ist.

Verfügbarkeit der Kommunikationsinfrastruktur ist daraus seit langem ein Kernelement der Betriebskontinuität und entsprechend berücksichtigt. Ein früher Ansatz war das Corporate Network Austria, auch

unabhängige Netzwerkanbindungen sind in Ressorts Standard, oder sind direkte Glasfaserverbindungen zwischen Ressorts verfügbar bzw. auch Internet Exchanges mit einer Möglichkeit der Abkopplung in einen Inselbetrieb im Notfall.

Diese schon traditionell länger gegebene Berücksichtigung der Betriebskontinuität im Datenaustausch heißt aber nicht, dass dies bzw. die Methoden nicht laufend zu hinterfragen sind und auch bei neuen Technologien neu zu bewerten ist, ob sich Annahmen mit der Infrastruktur nicht ändern. Ein schon etwas in die Jahre gekommenes Beispiel sind Ausfälle von Telefon-, Mobiltelefon- und Internet-Kommunikation im November 2004 über mehr als einen Tag vor allem in Wien, jedoch mit bundesweiten Auswirkungen. Damals wurde erst aus einem Ausfall nach Update eines Cross-Connectors der Telekom im Arsenal offensichtlich, dass eine Annahme redundanter (damaliger) SDH Ringe und die Annahme bekannter Leitungswege falsch war. Trotz paralleler Anbindung über unterschiedliche Anbieter war nicht bewusst, dass der betroffene Cross-Connector als gemeinsame Komponente singulärer Ausfallspunkt großflächiger Infrastruktur war. Das veraltete Beispiel, das in der Form nicht mehr anwendbar ist, dient der Illustration, dass aus Änderung der Technologien wie mit jüngerem Beispiel Software-definierte Netzwerke oder die bei 5G mit stark Cloud-basiertem Management oder Software-bestimmter Konfiguration auch andere Ausfall-Vektoren bestehen können, wie auch das Internet zwar in sich robust mit Redundanzen ist, eine Beeinträchtigung wesentlicher Komponenten wie DNS oder Core-Router auch großflächigere Ausfälle nach sich ziehen kann.

Öffentliche Kommunikationsnetzwerke sind robust und haben ein hohes Maß an Ausfallssicherheit. Der sehr hohen Abhängigkeit der öffentlichen Verwaltung von der Datenübertragung ist aber über deren laufende Beachtung der Ausfallsmöglichkeit zu begegnen, wo alternative Anbindungen und Routen, nach örtlicher Situation Direktverbindungen, oder auch alternative Technologien Mitigatoren darstellen.

3.5. Cloud-Services

Die Nutzung öffentlicher Clouds durch die öffentliche Verwaltung ist noch beschränkt, insbesondere bei missionskritischen Prozessen oder personenbezogenen Daten. Gründe sind trotz Kostendrucks oder hoher Verfügbarkeit und hoher Performanz vor allem auch Fragen der Vergabe oder rechtliche Bedenken zu Datenschutz oder dem US CLOUD Act.

Selbst wenn die Nutzung von Cloud noch gering ist, ist die Beschäftigung damit im Sinne digitaler Souveränität geboten, schon da mobile Endgeräte und Apps typisch auf Cloud aufbauen und oft intensiv nutzen. Auch ist bei standardisierten Diensten der Kostendruck beachtlich, wie auch Cloud-Strategien anderer Staaten wie rezent Frankreich 2021 Argumentationsdruck über eine Hypothese der Lösung von Fragen der Informationssicherheit oder rechtlicher Bedenken aufbauen, nachdem diese Fragen in anderen europäischen Staaten als ähnlich angenommen werden müssten.

In öffentlichen Clouds sind Hyperscaler wie Amazon, Microsoft Azure oder Google für standardisierte Dienste massiv am Markt agierend, gleichzeitig sind diese als US Anbieter jene, wo der CLOUD Act zur Datenübermittlung an US Behörden greift. Abhängigkeiten entstehen zu diesen nicht unbedingt aus technischer Natur, nachdem Lösungen Azure oder auch AWS mit Outposts auch lokal (on-premise) lauffähig sind, sondern aus dem Kostenvorteil der hochskalierenden Infrastruktur der Betreiber selbst.

Nationale Mitigations-Strategien zu Abhängigkeiten von großen öffentlichen Clouds sind on-premise Technologien, zumal moderne Rechenzentren Cloud-Technologien ohnehin nutzen bis hin zu nationalen Clouds wie die Bundescloud in Deutschland, wo sich aber Kosteneffekte nur national potentiell nicht in dem Maß einstellen können, wie sie bei den Hyperscalern gegeben sind. Höhere Skaleneffekte sind über mehrere Staaten oder europäische Ansätze erreichbar, allen voran das GAIA-X Projekt mit dem Ziel einer europäischen Dateninfrastruktur.

3.6. Home-Office

Mit der Covid-19 Pandemie wurde Home-Office auch in der öffentlichen Verwaltung ein stärkeres Thema, das aus den Erfahrungen und mittlerweile der Erwartungshaltung der Mitarbeiterinnen und Mitarbeiter in der einen oder anderen Form über die Pandemie hinausgehen wird. Eine Abhängigkeit entsteht daraus dadurch, dass dessen Umsetzung die Bereitstellung der technischen Möglichkeiten erfordert. Falls damit auch Reduktionen der Büroflächen etwa über Desk-Sharing einhergeht, wird Home-Office aus für alle Mitarbeiterinnen und Mitarbeiter nicht mehr ausreichenden Flächen zur Notwendigkeit zur Aufrechterhaltung des Betriebs.

Im Sinne digitaler Souveränität ist der Punkt Home-Office etwas abgesetzt, da es weniger fremdbestimmt ist, als etwa die Notwendigkeit von Software oder Betriebssystemen und faktisch dominanten Systemen. Gleichzeitig hängt funktionierendes Home-Office an technischen Möglichkeiten wie der internen Kommunikation über Videokonferenzen, homogener externer Erreichbarkeit wie mit Unified Communication, aber auch stabile Zugänge zu den Betriebsmitteln über VPN.

Die Anforderungen eines Home-Office im Regelbetrieb unterscheiden sich nicht grundsätzlich von denen aus der Pandemie, nach zwei Jahren mehr oder weniger laufendem Home-Office in der Pandemie lässt sich dieses auch fast schon als Regelbetrieb bezeichnen. Ein Unterschied kann aber darin gesehen werden, dass aus der zu Beginn der Pandemie kurzfristig aufgeprägten Notwendigkeit der Kontaktvermeidung und der allenfalls bestandenen Annahme einer früheren Rückkehr von interimistischer Situation ausgegangen wurde und damit Kompromisse oder kurzfristige Lösungen argumentierbar waren, die in dauerhafter Situation nicht mehr unbedingt zu halten wären.

Die Zugänge zu Betriebsmitteln über VPN produzieren keine direkte Anhängigkeit, zumal VPN sowohl in Betriebssystemen unterstützt ist, als auch eine Reihe an Produkten besteht. Es ist für einen dauernden Betrieb vor allem Performanz am Zugangspunkt wesentlich, wo aus der intensiven Nutzung während der Pandemie Erfahrungen bestehen sollten.

In den Audio- und Videokommunikationslösungen sind die Überlegungen zu Anwendungs-Software als Mitigation von Abhängigkeiten grundsätzlich anwendbar (vgl. Abschnitt 3.3), wobei in kommerziellen Lösungen wie Microsoft Teams über homogene Integration in die Produktfamilien wie etwa in Outlook Produktbindungen und damit Abhängigkeiten gestärkt werden. Es gibt aber hinreichend alternative Lösungen, auch in Open Source. Zusätzlich zur Anwendungskomponente sind, von peer-to-peer Ansätzen für kleinere Gruppen abgesehen, die Serverelemente zu betrachten. Hier sind on-premise gehostete in der Informationssicherheit einfacher zu bewerten, für Cloud-Lösungen sind Überlegungen vergleichbar zu Abschnitt 3.5 anstellbar.

4. Vermeidungsansätze

In diesem Abschnitt werden die zuvor skizzierten Strategien zur Vermeidung von Abhängigkeiten und damit Erlangung oder zumindest Verbesserung der digitalen Souveränität kategorisiert. Dabei wird explizit kein Erreichen einer autarken Situation, das heißt das durchgängige Erstellen unter nationaler Kontrolle mit nationalen Ressourcen, Entwicklung oder Produkten, verstanden. Wenngleich dies auch Strategie in einigen Elementen sein kann, ist digitale Souveränität auch gegeben, wenn Alternativen zu Herstellern hinreichend verfügbar sind.

Die genannten Kategorien schließen sich nicht gegenseitig aus, vielmehr können Strategien auf mehreren aufbauen.

4.1. Zugriff auf nationale Kompetenz und deren Ausbau

Wenngleich Österreich nicht alle Schichten der für die öffentliche Verwaltung notwenigen Informationstechnologie selbst abdecken kann, gibt es Stärkefelder, wo dies sehr wohl der Fall ist. So sind wesentliche Elemente des E-Government selbst entwickelt, besteht hohe Kompetenz in der Informationssicherheit sowohl aus dem akademischen Umfeld wie in einschlägigen Organisationen, oder sind leistungsfähige Rechenzentren unter staatlicher Kontrolle. Selbst wenn diese selbst intern Abgängigkeiten wie in den zuvor beschriebenen Bereichen haben können, ist damit ein gutes Maß an Eigenständigkeit gegeben.

Halten der Eigenständigkeit, wo hohe Qualität gegeben ist, und deren Ausbau in strategisch wichtigen Bereichen verhindert Abhängigkeiten. Um dies für die öffentliche Verwaltung auch nutzen zu können, ist in den Ressorts eigene digitale Kompetenz notwendig, nicht zuletzt um als Basis der Unabhängigkeit die Interessensfreiheit der unterstützenden Einheiten auch selbst einschätzen zu können.

4.2. Offene Schnittstellen und anerkannte Standards

Ein Grundsatz, der in den E-Government Strategien von Beginn verfolgt wurde, ist Austauschbarkeit von Komponenten dadurch, dass offene Schnittstellen vorgegeben werden, die auf anerkannten Standards aufbauen. Es erlaubt dies den Wechsel von Anbietern, wie auch technologischen Fortschritt über ein Ersetzen von Elementen einzubringen.

Ein Bekenntnis zu Standards bedarf auch entsprechender Einschätzung und Technologiebeobachtung, zumal die schiere Existenz einer Norm im dynamischen Umfeld der Informationstechnologien bei teils konkurrierenden Standardisierungsbemühungen noch nicht deren breiten Aufgriff garantiert. Auch können Standards von Interessen einzelner Segmente der Industrie getrieben sein, was erst wieder Abhängigkeiten schaffen kann. Um dies einschätzen zu können, bedarf es entsprechenden Domänenwissens, was eigene Kompetenz notwendig macht (vgl. vorigen Abschnitt 4.1 zu Kompetenz in strategisch wichtigen Bereichen).

4.3. Alternative Produkte und Open Source

Mitigation der Abhängigkeit von einem, potentiell dominanten Hersteller ist der gezielte Wechsel auf Alternativen. Aus Kostengründen, aber insbesondere auch wegen der offenen Entwicklungsmöglichkeit und um sich von marktbeherrschenden Herstellern keine unvorteilhaften Lizenzbedingungen aufzwingen zu lassen, sind Open Source Lösungen ein valider Ansatz.

In der Auswahl eines Produktes sind Interoperabilität und Konformität zu Standards (vgl. Abschnitt 3.2), aktive Wartung durch die Entwicklergruppe und deren laufende Weiterentwicklung des Produkts wesentlich. Auch hier macht es Sinn, Alternativen zu erwägen, um bei Auslaufen Ersatz zu haben.

4.4. Best Practices und Kooperation mit anderen Staaten

Mit Open Source Produkten können sich Abhängigkeiten insofern einstellen, als man auf längerfristige Bereitschaft der Community angewiesen ist, das Produkt weiter zu entwickeln. Es empfiehlt sich, von anderen Staaten bereits eingesetzte Komponenten im Sinne eines Best Practice zu erwägen und deren Erfahrungen zu berücksichtigen. Dies ist etwa beim Bundesclient im Erproben der deutschen Phoenix Suite erfolgt.

Bei strategisch wichtigen Funktionsblöcken wie Office Software kann die Kooperation mit anderen Staaten Sinn machen, um im gemeinsamen Einsatz einer Lösung Hebeleffekte zu erzielen. Über abgestimmte Interessen ließen sich Entwicklungen auch gemeinsam und damit kostengünstiger umsetzen und so auch internes Know-How zum strategisch wichtigen Produkt selbst aufbauen, um notfalls ein schwindendes Interesse der bisherigen Entwickler-Community kompensieren zu können.

4.5. Gesamteuropäische Lösungen

In Bereichen, in denen massive Dominanz von Herstellern oder ganzer Sektoren nicht-europäischer Provenienz gegeben ist, können sich Abhängigkeiten besonders unvorteilhaft entwickeln, da derartige Marktbeherrschung nicht nur von den Herstellern selbst, sondern auch staatlich strategisch genutzt werden könnte. Starke nicht-europäische Vorherrschaften sind im Bereich der Endgeräte, insbesondere auch im Mobilbereich, bei Infrastrukturkomponenten, oder bei Betriebssystemen gegeben. Europäisch konsolidierte Positionen und Vorgehen sind bei derart massiven Dominanzen etwa über die Marktmacht des EU Binnenmarktes geeigneter, negative Abhängigkeiten abzuschwächen, als einzelstaatliche Ansätze.

Bereiche wo europäisches Vorgehen erfolgversprechend ist, sind die Interoperabilität, für die öffentliche Verwaltung etwa der europäische Interoperabilitätsrahmen EIF, insbesondere aber auch gemeinsame Vorgaben und Standards zur Informationssicherheit. Bei letzterem kann sich der Cyber Security Act als gemeinsames Mittel erweisen, Zertifizierung als für kritische Funktionsblöcke höchstwertige Form der Standarddurchsetzung auf EU-weit breit abgestimmter Basis umzusetzen.

5. Strategieentwicklung und Vorgehensvorschlag

Diese Arbeit hat bestehende oder mögliche Abhängigkeiten, die die öffentliche Verwaltung in der Informationstechnologie hat oder haben kann, in Bereichen aufgezeigt und Ansätze zu Mitigation solcher Abhängigkeiten im Sinn der Erlangung oder zumindest Verbesserung digitaler Souveränität kategorisiert. Ziel war es, den Diskurs einer weiteren, strukturierten Vorgehensweise zur digitalen Souveränität vorzubereiten.

Um eine solche strukturierte Vorgehensweise zu entwickeln, müssen Abhängigkeiten bekannt sein, das heißt systematisch erfasst werden. Dies heißt nicht, dass Schmerzpunkte wie Abhängigkeiten bisher nicht schon bewusst waren oder dass nicht bisher Initiativen zu deren Linderung gesetzt worden wären. Es geht vielmehr darum, der öffentlichen Verwaltung schon bekannte oder dieser allenfalls noch weniger klare Abhängigkeiten in einer Landkarte aufzuzeigen, um damit systematisch analysieren zu können, wo die größten Risken bestehen und damit Handlungen priorisiert zu setzen. Die in Abschnitt 3 erfassten Bereiche zusammen mit den in Abschnitt 2 skizzierten Quellen solcher Abhängigkeit können als ein Startpunkt dienen.

Das Vorgehensmodell lehnt sich an die Ziele und Handlungsfelder der deutschen Konferenz der IT-Beauftragten der Ressorts [4] an, wobei dies insofern angepasst wurde, als in Österreich zur Koordination der Verwaltungsebenen aus dem E-Government mit der Bund, Länder, Städte und Gemeinden (BLSG) Koordination bereits gut funktionierende Strukturen bestehen.

Dementsprechend wäre der Vorgehensvorschlag angelehnt an die Handlungsfelder aus [4]:

- Systematische Analyse von Abhängigkeiten
- Systematische Analyse bestehender Initiativen zur Mitigation
- Priorisierung und strategische Lösungskonzeption
- Entscheidung und Umsetzung

In der systematischen Analyse von Abhängigkeiten sollte eine Landkarte wesentlicher Abhängigkeiten erstellt werden. Als Methodik bietet sich im Vorfeld eine Literaturrecherche vergleichbarer Vorhaben anderer Staaten an, so hat etwa [3] den Software-Stack der deutschen Bundesverwaltung analysiert,

gefolgt von einer Studie mit Interviews mit einigen relevanten Spielern, d.h. einigen Ressorts, dem BRZ und Ländern.

Weiters sollten in Österreich bereits bestehende Initiativen erfasst werden. Dies kann zusammen mit der Studie im Rahmen der vorgenannten Erfassung der Abhängigkeiten erfolgen, zumal eine Einheit, der eine solche bewusst ist, potentiell schon Überlegungen oder konkrete Schritte zur Beseitigung angestellt hat. Jedenfalls wäre dabei die AG Bundeclient einzubeziehen, die sich für Endgeräte bereits damit befasst.

Eine Erfassung von Schmerzpunkten und bestehenden Initiativen oder Plänen soll nicht zuletzt ein Bild ergeben, welcher Ist-Stand in der digitalen Souveränität besteht. Ein gewünschter Soll-Stand ist eine strategische Entscheidung, zumal nicht jede erfasste Abhängigkeit auch eine relevante Beeinträchtigung des selbstbestimmten staatlichen Handelns in der digitalen Welt sein muss. Hier scheint Befassung der BLSG geboten, um ein Zielbild zu entwickeln, das von allen Verwaltungsebenen getragen werden kann, um dann im Vergleich des Ist-Stands zu diesem Zielbild eine Sicht auf Handlungsbedarf zu haben.

Die Entscheidung des Zielbildes kann ein Strategiepapier Digitale Souveränität mit Terminen zu deren Erreichung sein, wo wiederum BLSG eine Priorisierung vornehmen sollte, um zur konkreten Umsetzung die Arbeitsgruppen beauftragen zu können.

Referenzen

[1] Bundesministerium für Wirtschaft und Energie, Schwerpunktstudie Digitale Souveränität, Bestandsaufnahme und Handlungsfelder, 2021

[2} Kompetenzzentrum öffentliche IT. Digitale Souveränität, ISBN 978-3-9818892-2-2, 2017.

[3] strategy&, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, Abschlussbericht 2019.

[4] Konferenz der IT-Beauftragte der Ressorts, Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung, Eckpunkte – Ziel und Handlungsfelder. Beschluss Nr. 2020/01 vom 31. Jänner 2020.

[5] Bitkom, Digitale Souveränität – Positionsbestimmung und erste Handlungsempfehlungen für Europa, 2015.